Full-duplex quantum coherent communication

Rupesh Kumar[1], **Tim Spiller**[1]
[1] *Quantum Communications Hub, Department of Physics, University of York, York YO10 5DD, UK*
e-mail: rupesh.kumar@york.ac.uk

ABSTRACT
High bandwidth requirements for data communications are currently being met by classical coherent communication using multi-level modulation of amplitude and phase of light. Alternatively, down at the level of quantum signals, coherent communication enables establishment of cryptographic keys between two legitimate users, and shows higher key exchange throughput compare to single-photon-based systems. In this work, we will examine the feasibility of full duplex quantum coherent communication, where both the transmitter and the receiver engage in quantum signal recovery as well as secure key generation.

Keywords: Continuous variable (CV) quantum key distribution (QKD), shot-noise limited coherent detection, Transmitted local oscillator, Local local oscillator.

1. INTRODUCTION

In classical communications that relay on threshold detectors for signal recovery, the data carrying bandwidth is limited by the signal repetition rate. For example, the On-Off Keying (OOK) format carries one bit per signal pulse—typically with zero amplitude for bit value 0 and high amplitude for bit value 1. Coherent communication using amplitude and phase modulation, referred to as quadrature modulation, offers data transfer with unprecedented bandwidth, both in fibre optic networks (10G/100G) and free-space communications. Instead of detecting the signals with a single threshold photo-diode, coherent communication requires detectors that can resolve quadratures of the signals[1]. This is achieved by coherent mixing on a symmetric beam splitter of the incoming signals with a strong reference signal—called the local oscillator (LO)—and deducing the quadrature information from the mixed signal outputs. In the case of multi-amplitude only modulation format, a direct detection of one of the mixed signal outputs with a photo-diode reveals the data itself, provided that the input signal strength is adequate. With more complex formats such as Quadrature Amplitude Modulations (QAM), both quadratures have to be measured. This is performed by converting the mixed signal outputs to photo currents using a pair of photo-diodes, followed by the amplification of the difference of the photo-currents. Data post-processing on phase and clock recovery reveals the data bits, thereafter. Importantly, the input signal to this coherent detector must be above a permissible amplitude in order to deliver error free data communication. The tolerance to errors can be increased with forward error corrections methods. In this paper we consider the case of coherent communication with signals at the lowest possible—quantum—level. In principle, this approach cannot accurately transport data bits from a transmitter to receiver, due to the inherent quantum uncertainties associated with the quadratures values. However, such quantum uncertainties instead facilitate the generation of secure cryptographic keys.

2. QUANTUM COHERENT COMMUNICATION

Cryptographic key exchange using quantum properties of light is referred to as Quantum Key Distribution(QKD). Based on the dimensionality of the quantum signal states of light used, QKD is categorized into discrete variable (DV)-QKD and continuous variable (CV)-QKD. Similarly to OOK, DV-QKD relies on on-off detection at the single photon level, where each detection event contributes to a single cryptographic key bit. In contrast, since a single classical coherent communication quadrature can carry multiple bits, for CV-QKD each measurement can therefore contribute to more than just a single key bit. This works only at shorter transmission distances, whereas at longer distances the secure key rate drops to less than one bit per signal pulse due to the decreasing signal-to-noise ratio.

Electronic noise from the photo-diodes and current amplifiers is the major limiting factor for achieving high signal-to-noise ratio in coherent communications. In classical coherent communication, this is overcome by using strong signals, whilst in quantum communications it is addressed by selecting detectors and amplifiers with lower electronic noise at the cost of reduced detection bandwidth—down from GHz to MHz. This makes the detector sensitive to vacuum noise (shot-noise) associated with the quantum signals. The uncertainty in measurements due to the vacuum noise brings security to the quantum signal transmission, that in turn enables secure cryptographic key generation. A difference to be noted is that, in classical coherent communications, a polarisation diversity measurement is used for compensating polarisation drift of the signal. This would induce extra loss in signal strength, which would decrease the secure key rate in CV-QKD systems. Therefore, in CV-QKD single polarisation measurement is implemented with active polarisation control.

CV-QKD, and coherent communication generally, shows high tolerance to noise photons originating from other sources. This makes CV-QKD a promising candidate for cryptographic key exchange in noisy environments,

such as dense wavelength division multiplexed (DWMD) fibre networks and free-space communications in daylight. The small footprint of a CV-QKD system makes it highly suitable for photonic integrated circuit (PIC) approaches without detector cooling. Such cooling is generally necessary for single-photon-based DV-QKD systems. Classical coherent systems benefit significantly from a PIC approach, where it is common to have a full transceiver set-up on a single chip. This realises a full duplex coherent communication system, where each user can transport data to each other. Such a transceiver concept can be also applied to CV-QKD. In this paper we will consider the feasibility of this approach, and examine the characteristics and achievable secure key rate.

3. Performing CV-QKD

In this section we will consider the requirements for performing CV-QKD with coherent signal modulation and detection. We consider the transmitter (Alice) and receiver (Bob) architectures are analogous to classical coherent systems, except that: (i) Alice can attenuate the signal strength down to vacuum level and calibrate it with respect to shot-noise; Bob can utilise (ii) a fast optical switch to assist the shot-noise measurement, and (iii) a shot-noise sensitive linear coherent receiver. With these characteristic modifications to a coherent transceiver, we consider the following approach applied to CV-QKD. Basic set-ups for Alice and Bob are shown in Fig.1 (a) and (b), respectively.

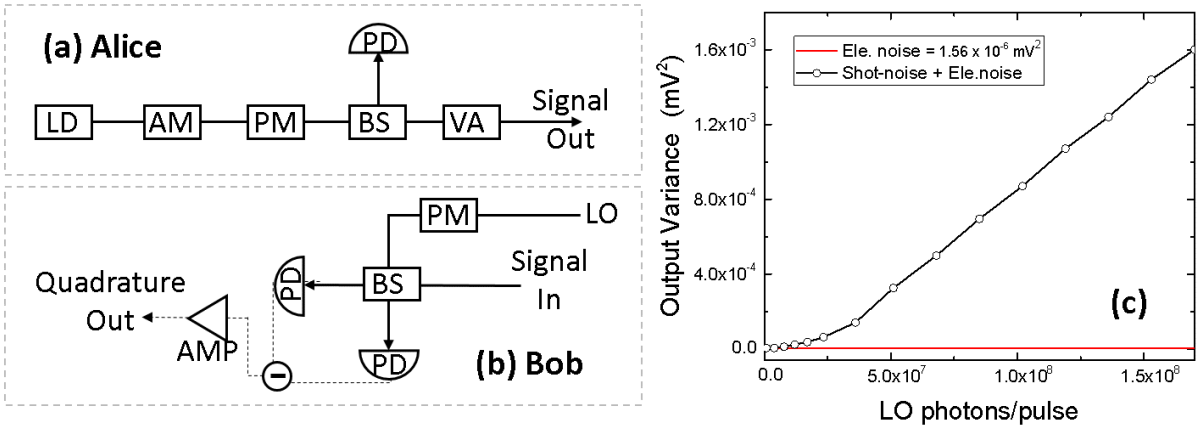

Figure 1. *(a) A simplified Alice set-up. An intense pulse from laser diode (LD) is amplitude (AM) and phase (PM) modulated. A beam splitter (BS) splits a part of the signal to the photo-diode (PD). The output signal is highly attenuated to the quantum level by a variable attenuator (VA). (b) Bob's homodyne detection set-up for measuring one of the quadratures (at a time). The LO is either sent from Alice or locally generated. A phase modulator (PM) for the LO sets 0 phase for X- and 90 degrees for P-quadrature measurement. The outputs of the beam splitter (BS) are converted into photo-currents by photo-diodes and their difference is amplified to give the quadrature value (as set by the PM). (c)Output variance of a shot-noise limited homodyne detector.*

3.1 Shot-noise measurement

As a requirement to have sensitivity to vacuum noise, the electronic noise of the CV-QKD receiver must be much lower than that of a classical coherent receiver. Such CV-QKD receivers are called shot-noise limited. It is also required that the detection output shows linear response to the input signal variance—an assumption under the Gaussian linear model used for the protocols[2]. Fig.1(c) shows the linear response of such a shot-noise limited receiver. A strong LO brings the detector into shot-noise sensitivity.

Estimation of shot-noise variance is performed in order to normalise the quadrature values sent by Alice and received by Bob such that they have mutual agreement on the absolute quadrature values, which later can be converted into key bits. Shot-noise variance is the output variance of the coherent receiver which is measured with reference to the LO power. There are a few techniques to estimate the shot noise variance, all of which assume that the input signal to the receiver is vacuum or known, against a set attenuation. In a simple procedure shot-noise variance is estimated from LO intensity against pre-calibrated values. The most promising technique is to block the signal with a fast optical switch and measure the shot-noise variance in real time. This helps not only to account for slowly varying measurement mean values (which affect the estimation of the shot-noise variance), but also to block noise photons, from DWDM channels or from background, during measurements.

3.2 Calibration of quantum signals

The quadratures of the signals at the output of Alice are calibrated with a shot-noise limited coherent receiver with known detection efficiency. This is done without a channel in between the Alice and Bob systems, or with a

channel of known attenuation. The later method opens a security loophole as an eavesdropper could manipulate the channel parameters and thus control the calibration process, in particular CV-QKD systems deployed in the field. The signal variance measured and normalised to the shot-noise variance is made to correlate to the feedback photo-diode's (PD) output, shown in Fig.1(a). It is important to note that the signals are modulated at higher intensity and then brought down to the quantum level by means of a variable attenuator (VA) at the output. This leaves adequate signal strength to be detected by the photo-diode. During a QKD protocol run, the signal variance is evaluated directly from the photo-diode's output.

3.3 The QKD protocol run

During the protocol execution, Alice generates coherent states $|\alpha_A\rangle = |X_A + iP_A\rangle$ and sends these to Bob through the quantum (communication) channel. The quadratures, X_A and P_A, are randomly chosen from sets as defined by the protocol. For example, in discretely modulated CV-QKD protocols such as four-state protocols, the quadrature values are selected from the binary sets $\{X_A, -X_A\}$ and $\{P_A, -P_A\}$. In Gaussian modulated coherent state (GMCS) protocols[3], the quadratures are drawn from sets of normally distributed random variables $\mathcal{N}\{0, V_A\}$, of zero mean and variance V_A. In this analysis we consider a GMCS protocol. Bob measures the quadratures with respect to the LO, using a shot-noise limited homodyne (or heterodyne) coherent receiver. The transmittance T and the excess noise ξ characterise the quantum channel. These can be obtained from the transmitted and received quadrature covariances, $\eta T V_A$ and $\eta T V_A + N_0 + \eta T \xi + v_{ele}$, respectively. Here, η is the detection efficiency of Bob, N_0 is the shot-noise variance and v_{ele} is the electronic noise variance. These conditions apply for both X_B and P_B quadrature measurements. The secure key generation rate can be estimated from knowledge of the channel parameters, T and ξ. The secure key rate in the asymptotic (large key) limit, under collective eavesdropping attacks and with reverse reconciliation, is $\gamma(\beta I_{AB} - \chi_{EB})$. Here, γ is the fraction of quadrature data used for secure key generation and β is the reconciliation efficiency. I_{AB} is the mutual information between Alice and Bob and χ_{EB} is the eavesdropper's (Eve's) accessible information—Holevo bound—to the quadrature measured by Bob. A detailed derivation of this secure key rate is given in [2]. From the channel parameter estimation, provided that the level of excess noise ξ is below the null key threshold, Alice and Bob can estimate the secure key rate. They can then proceed to error correction and privacy amplification, in order to generate unconditionally secure keys.

4. Transmitted Local Oscillator

The LO serves various purposes. It provides a phase reference for the quadrature measurements at Bob, such that Alice and Bob have identical quadrature values for key generation. The strong coherence of the LO with respect to the signal helps to reduce the impact of noise photons in the quadrature measurements. The LO also provides amplification to the signal quadrature, proportional to the LO amplitude and given by $2\sqrt{I_{LO}}X_B$, where I_{LO} is the intensity of the LO. In conventional GMSC demonstrations, the LO is sent along with the signal. This is now referred to as a transmitted LO (TLO) scheme[2]. Since the shot-noise variance is estimated with respect to the LO strength, in order to have lower electronic noise v_{ele}, LO power is required to be as high as possible without damaging and saturating the photo-diodes. Typically, the LO power is kept at 10^8 photons per pulse at Bob. This is not achievable at longer channel distances and higher repetition rates due to the peak power limitations of the transmitting laser at Alice. This is a potential problem for TLO-based approaches. More importantly, TLO schemes open a security loophole where Eve can manipulate the LO intensity and affect the shot-noise variance measurements, that in turn can mask the noise from her attacks. A proper countermeasure to monitor LO intensity fluctuations can neutralise this attack.

5. Local Local Oscillator

In order to obviate the attack on the TLO and to converge into the classical coherent detection scenario, a local local oscillator (LLO) scheme has been proposed in which the LO is generated from a second laser at Bob[4]. This is exactly the situation in classical coherent communication. However, a drift in mutual coherence of both lasers creates excess noise and limits the performance of the LLO scheme. Moreover, it is necessary to transmit a reference signal from Alice in order to lock the phase of the second laser during quadrature measurements. The phase-locking can either be performed during signal detection or later, during data post-processing. The excess noise in the most general LLO scheme is the phase noise ξ_{phase} given as $2V_A(1-e^{-V_{est}/2})$. Here V_{est} is the variance of the phase estimation, which derives from: (1) the phase estimation error of the reference pulse, $V_{error} = (\xi + 1)/I_{ref}$; (2) the phase drift between the reference and the signal due to the line width of the lasers, given by $V_{drift} = 2\pi(\Delta_A + \Delta_B)/f$; (3) the phase accumulated during the channel propagation, V_{ch}. Here I_{ref} is the reference pulse intensity, $\Delta_{A(B)}$ is the linewidth of the respective lasers and f is the repetition rate. These noise sourcess in LLO schemes limit the maximum transmission distance and secure key generation rate. A detailed noise estimation procedure is given in [4].

6. FULL DUPLEX SECURE KEY GENERATION

We consider a full-duplex CV-QKD system in both TLO and LLO schemes. In a full-duplex communication, each end of the communication channel has a pair of Alice and Bob systems. We consider these transceiver systems to be realised as PICs, as per the case of full-duplex classical coherent communication. Also, the operational wavelength of the transceiver module is set to be the same for both Alice and Bob. This requires, as per the classical full-duplex communication, two separate fibres to avoid noise photons from Rayleigh back-scattering due to LO or reference pulses. A plausible configuration is shown in Fig.2(a) for TLO and 2 (b) for LLO schemes. From the discussion in section 3, we can see there are major advantages of full-duplex coherent

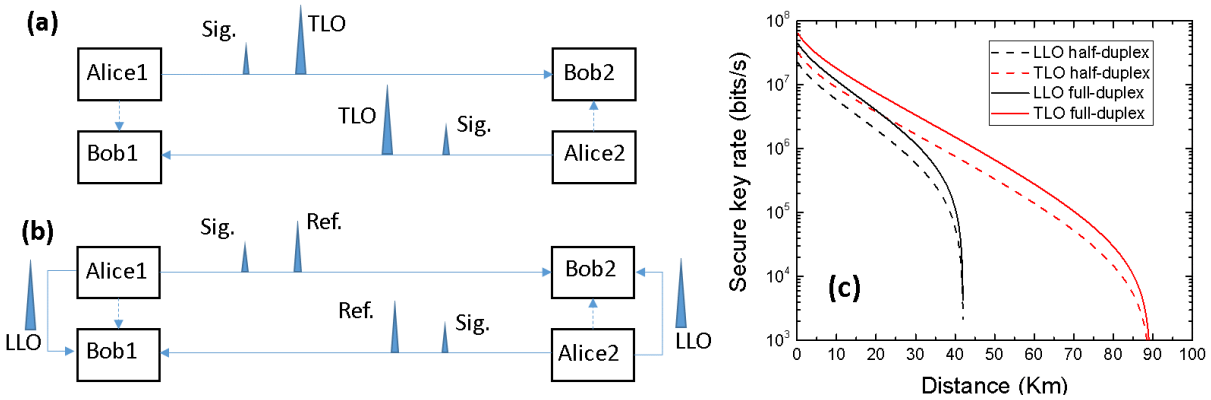

Figure 2. (a) A TLO scheme in full-duplex configuration. The Bob set-up is based on homodyne detection. Dotted lines show internal paths for signal calibration. (b) A LLO scheme in full-duplex configuration. (c) Estimated key rates of TLO and LLO full-duplex systems with various transmission distances. The following parameters are used: $\beta = 0.95$, $\eta = 0.6$, $v_{ele} = 0.1$, $V_A = 10N_0$, *total excess noise* $\xi_{LLO} = 0.1N_0$, $\xi_{TLO} = 0.05N_0$, $\Delta_{A(B)} = 1.9kHz$ *and 50MHz clock rate with* 90% *of samples used for key generation.*

communications for CV-QKD. First of all, in half-duplex CV-QKD systems, once the initial calibration prior to the field deployment has been done, it may be difficult to recalibrate the systems without bringing them together again in back to back configuration. Recalibration is necessary in order to avoid possible security loopholes that arise from system degradation. For example, fluctuations in: ambient temperature; electronic noise; spitting ratio of beam-splitters; attenuation set by the variable attenuator; biasing voltage of modulators; etc. These result in drift of the signal level from its calibrated value. In such situations, a receiver in the transceiver module can recalibrate the systems on site. Secondly, from the commercial point of view this makes the CV-QKD system more cost effective as it required to produce a single hardware system, requiring single system characterisation and bench-marking. As an obvious advantage, the key rate is doubled. Comparison of secure key rates from full-duplex TLO and LLO based CV-QKD systems is given in Fig.2 (c).

7. CONCLUSION

We have considered full-duplex secure key generation using CV-QKD systems. We have described the requirements for CV-QKD protocols to run and proposed advantages of having a full-duplex configuration in field-deployed systems. We also show the secure key generation rate for both TLO and LLO based systems under full-duplex configuration.

ACKNOWLEDGEMENT

We acknowledge funding from the UK Engineering and Physical Sciences Research Council (EPSRC) Grant no. EP/M013472/1.

REFERENCES

[1] K Kikuchi. Fundamentals of coherent optical fiber communications. *J. Light. Technol.*, 34:157, 2016.

[2] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A*, 76:042305, Oct 2007.

[3] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[4] Tao Wang, Peng Huang, Yingming Zhou, Weiqi Liu, Hongxin Ma, Shiyu Wang, and Guihua Zeng. High key rate continuous-variable quantum key distribution with a real local oscillator. *Optics Express*, 26:2793, 2018.